Segregated Wireless Network Infokit for Android Phone

Version 1.0

Contents

ANNEX A (SWN ACCEPTANCE USE POLICY)

This Acceptable Use Policy (AUP) is intended to protect the Ministry of Education, Singapore (henceforth referred to as the "MOE") and Schools (henceforth referred to as the "School") from the inappropriate use of the Internet.

The use of SWN@SSOE or GUEST@SSOE Wireless service (henceforth referred to as the"Service") constitutes the school acceptance of this AUP. The School is responsible for keeping itself informed of the current AUP in effect, including any revisions or updates, and for abiding by the terms of this AUP.

1. SWN Wireless Service shall only be used for lawful purposes, and School shall undertake the responsibilities to ensure such use complies with all applicable laws. The School is responsible for all use of wireless accounts, with or without the knowledge or consent of the School.
2. MOE reserves the right, at its sole discretion, with or without notice, to suspend or terminate the Service provided if the School or any guest user using School's Service or facilities, directly or indirectly:-
    - Sends, or facilitates the sending of, unsolicited bulk mail messages ("email spam") to any person or system in a way that could be expected to adversely impact MOE's network or facilities; or sends mail-bombs (masses of email or other data) to any person or system, propagates or replies to mail-bombs;
    - Uses the Service in a manner which is intended to abuse or to violate the property rights of others, including, without limitation, activities which result in the distribution of viruses, worms, time bombs, Trojan horses, or other destructive activities;
    - Uses the Service in a manner that infringes on the intellectual property rights of any third party or any rights of publicity or privacy;
    - Publishes or communicates material that is obscene, defamatory, trade libelous, unlawfully threatening or unlawfully harassing;
    - Uses the Service to attempt to break security, or in fact, breaks security of any computer network, or to access an account without authorization;
    - Uses the Service to conduct any other activities which MOE determines are injurious to its users, operations, or reputation;
    - Attempts to share or resell MOE service without MOE's express authorization; or
    - Uses bandwidth or disk space in excess of limits permitted in MOE IT policy (where applicable)
3. School must immediately notify MOE of any unauthorized use, and/or any breach, or attempted breach, of security known to School. School may not, through action or inaction, allow others to

use its network for illegal or inappropriate activities. MOE takes no responsibility for the security of the communications transmitted over Segregated Wireless Service.

4. MOE, in its sole discretion, will determine on a case-by-case basis what action will be taken in response to a violation of this AUP. MOE reserves the right to investigate suspected or alleged violations of this AUP, including gathering information from School, its guest users, and examining of material on MOE's servers.
5. MOE shall not be liable for any damages of any nature suffered by any School or any third party resulting in whole or in part from MOE's exercise of its rights under these policies.
6. MOE reserves the right to amend, alter, or modify this AUP at any time in its sole and absolute discretion. Any amendment or modification is effective when posted and any use of this Service after the posting of a modification or amendment will be considered acceptance of those modifications.
7. The School's Segregated wireless users shall be solely responsible for ensuring that their client software is suitable for their needs and it is compatibility for use with any equipment used by him or her, whether or not MOE introduces any changes to the Service

ANNEX B (SWN LOGON GUIDE)

To connect to the Segregated Wireless Network, the device must meet the prerequisite requirements stated below. As there would be no compliance or enforcement check on the requirements, so it is the user's duty/responsibility to ensure the following prerequisite are met and updated with the latest version.

1) Prerequisites:

I. Wi-Fi (802.11g/n) enabled

II. Web browser supported but not limited to:

   a. Internet Explorer

   b. Firefox

   c. Safari

   d. Google Chrome

III. Login Credentials

   a. Authentication via SSOE Active Directory credential. For SSOE users to logon using their IAMS logon.

2) Steps to Logon

Overview of wireless logon procedures:

i. Configure the device and connect to SWN wireless SSID. (SSID is set to broadcast)

ii. Launch the web browser and user would be greeted with the Segregated Wireless logon page.

iii. Acknowledge the user acceptable policy and terms and conditions and logon using IAMS userid & password.

iv. Upon successful logon, user would be redirected to the successful logon landing page.

v. User is required to download the SSL certificate from the hyperlink and install into their non-SSOE device for security compliance (One time installation per device).

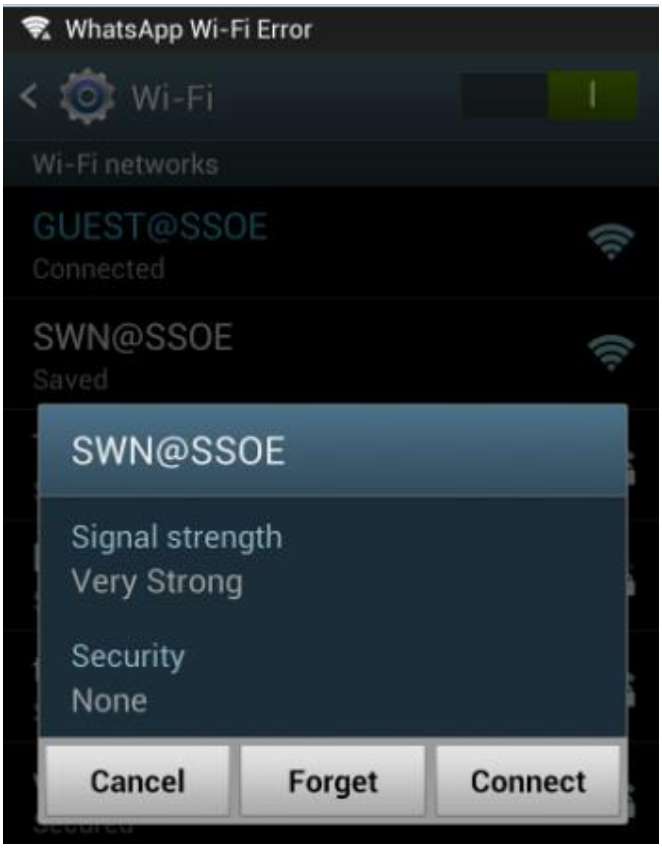
vi. Upon completed configuration, user can open a new browser to proceed with internet surfing.

Android Phone

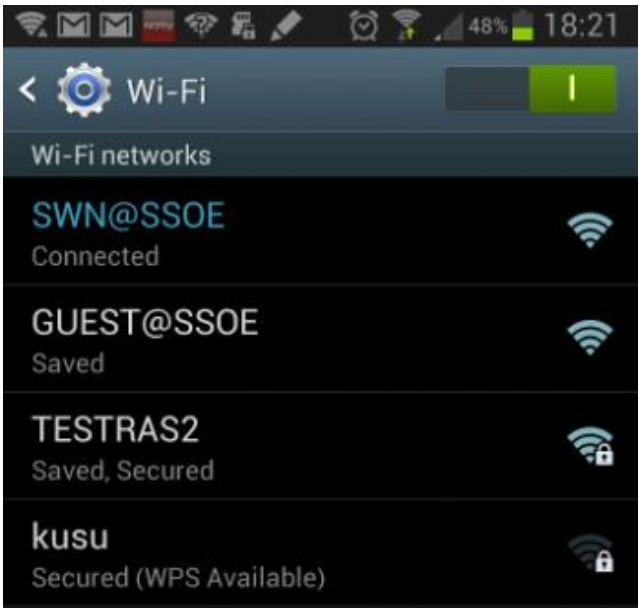
1. Locate and click on the “Settings” application.

2. Select and turn on the Wi-Fi

3. Scan for “SWN@SSOE” Network.

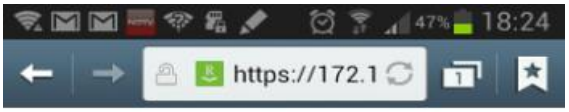


4. Click on “Connect”, the SSID would be highlighted upon successful connection.

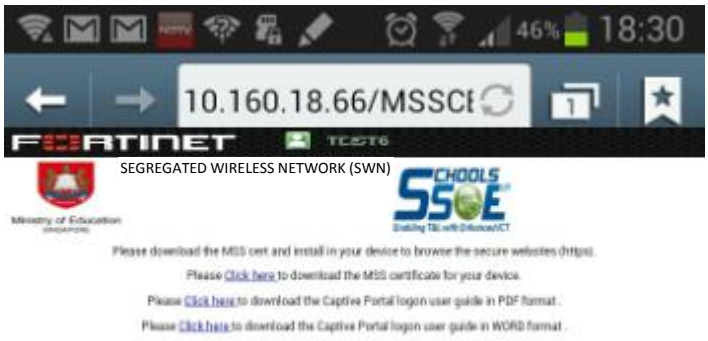


5. Locate and click on the “Internet” browser application.

6. User need to check on the checkbox to accept the (Acceptance Use Policy) & (Terms & Conditions) before key in the IAMS logon userid and password.

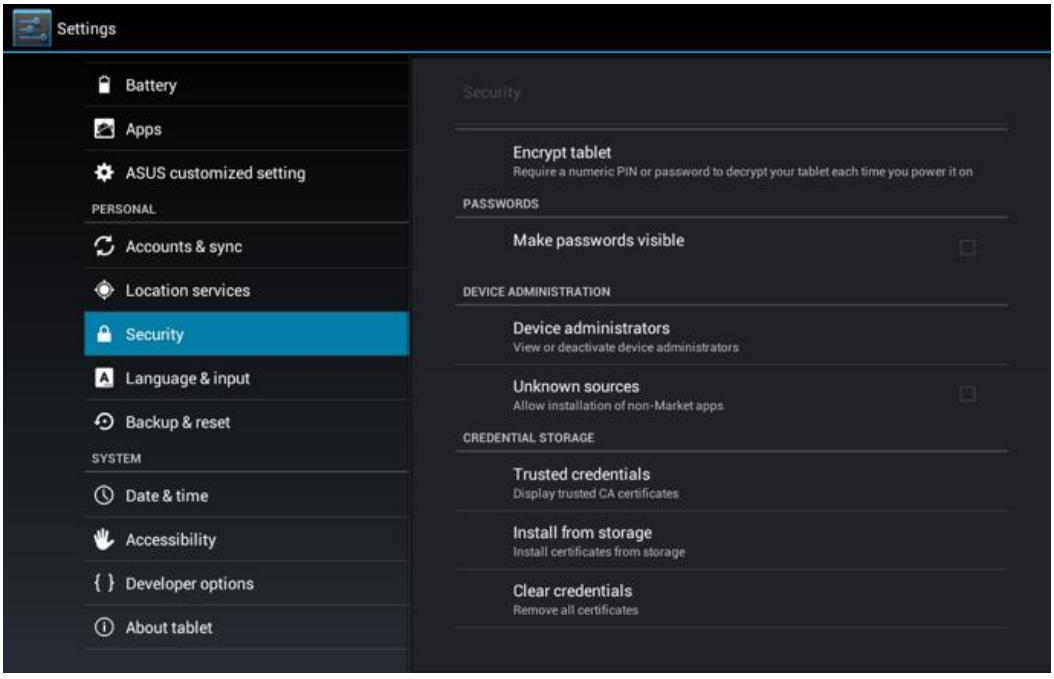


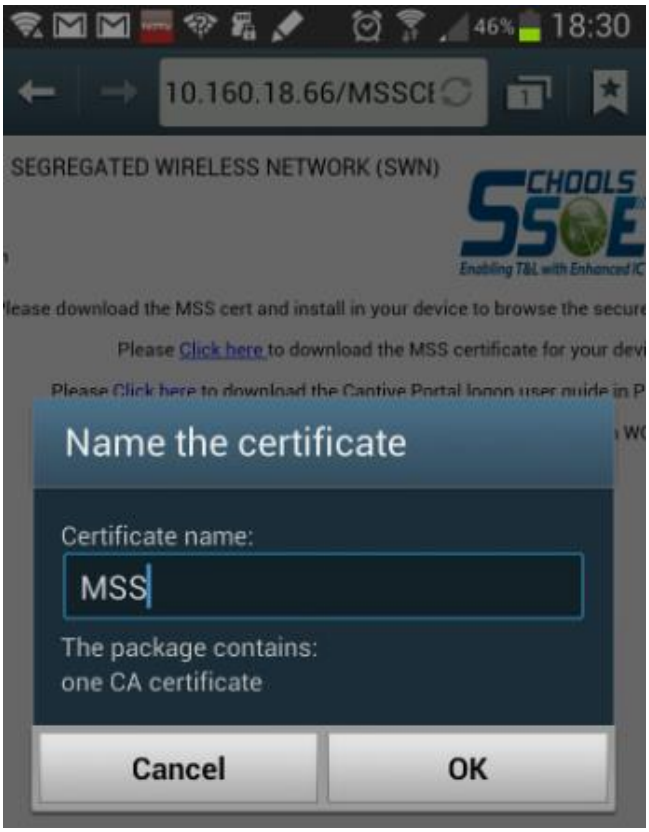
7. After successful logon, the browser would be redirected to the SWN landing homepage.



8. Click on the link to download the MSS certificate. A window will pop out to name the certificate. Key in “MSS” into the “Certificate name:” and click on the “OK” button.
(subsequent logon using the same device does not require the certificate installation)

9. If the MSS certificate is saved to storage, locate and click on the “Settings” application. Select “Security” and click on “Install from storage”. A window will pop out to name the certificate. Key in “MSS” into the “Certificate name:” and click on the “OK” button.





10. Add the SWN landing homepage (http://portal.swn.moe.edu.sg) into the web browser bookmark list. The logout bar would appear at the top of the SWN landing page for ease of logout.

11. The device is ready for internet access. To continue with internet web surfing, launch another browser window and proceed

ANNEX C (FAQS)

Q: My machine does not detect the SWN@SSOE SSID, how should I resolve it?

A: Make sure the device Wi-Fi is turn on, refer to the SWN logon guide to find out how to enable your wireless.

Q: Can I use the same account ID to access two (2) of my personal computing devices at the same time?

A: No, concurrent login is not allowed.

Q: I have forgotten my IAMS password, how to I reset my password?

A: For Student IAMS account, kindly approaches the student local administrator to reset the password. For Staff IAMS account, kindly approach the staff local administrator.

Q: I noticed that I am disconnected from the network after 30 minutes of inactive Internet activity? Is my account lockout?

A: No, as part of a security feature, your connectivity will be disconnected after 30 minutes of inactive Internet activity. Please log in again to regain your access.

Q: I cannot access some iPhone/Android application after successful logon?

A: Application behavior varies and depends on each developer. If the application is developed using none standard http & https port, it would be blocked.

Q: How can we change the SWN@SSOE account password?

A: The SWN portal does not support changing of IAMS password. The IAMS logon password is synchronized with the SWN logon password, changing your IAMS password is equivalent to changing your SWN@SSOE password. User can use an SSOE machine to change the IAMS password.